

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 1. (Currently amended) A method for managing a database system,  
2 comprising:  
3 receiving a command to perform an administrative function involving an  
4 object defined within the database system;  
5 determining if the object is a sensitive object that is associated with  
6 security functions in the database system, wherein the sensitive object and only  
7 the sensitive object is encrypted in the database system, wherein the sensitive  
8 object can include a sensitive row within a table in the database system, wherein  
9 the sensitive row contains sensitive data, and wherein other rows in the table need  
10 not contain sensitive data;  
11 wherein the sensitive object can include one of:  
12 a sensitive table containing sensitive data in the database  
13 system, and  
14 an object that represents a sensitive user of the database  
15 system who is empowered to access sensitive data,  
16 whereby an administrator cannot become a sensitive user  
17 and thereby obtain access to sensitive objects indirectly;  
18 if the object is not a sensitive object, and if the command is received from  
19 a normal database administrator for the database system, allowing the  
20 administrative function to proceed; and  
21 if the object is a sensitive object, and if the command is received from a  
22 normal system administrator, disallowing the administrative function.

1 2. (Original) The method of claim 1, further comprising:

2 receiving a request to perform an operation on a data item in the database  
3 system;

4 if the data item is a sensitive data item containing sensitive information  
5 and if the request is received from a sensitive user who is empowered to access  
6 sensitive data, allowing the operation to proceed if the sensitive user has access  
7 rights to the data item; and

8 if the data item is a sensitive data item and the request is received from a  
9 normal user, disallowing the operation.

cl

1 3. (Original) The method of claim 2, wherein if the data item is a sensitive  
2 data item, if the operation is allowed to proceed, and if the operation involves  
3 retrieval of the data item, the method further comprises decrypting the data item  
4 using an encryption key after the data item is retrieved.

1 4. (Original) The method of claim 3, wherein the encryption key is stored  
2 along with a table containing the data item.

1 5. (Original) The method of claim 4, wherein the encryption key is stored  
2 in encrypted form.

1 6. (Canceled).

1 7. (Original) The method of claim 1, wherein if the object is not a sensitive  
2 object, and if the command to perform the administrative function is received  
3 from a security officer, the method further comprises allowing the security officer  
4 to perform the administrative function on the object.

1 8. (Original) The method of claim 1,  
2 wherein the database system includes a number of sensitive data items;  
3 and  
4 wherein only specific sensitive users are allowed to access a given  
5 sensitive data item.

1 9. (Currently amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for managing a database system, the method comprising:  
4 receiving a command to perform an administrative function involving an  
5 object defined within the database system;  
6 determining if the object is a sensitive object that is associated with  
7 security functions in the database system, wherein the sensitive object and only  
8 the sensitive object is encrypted in the database system, wherein the sensitive  
9 object can include a sensitive row within a table in the database system, wherein  
10 the sensitive row contains sensitive data, and wherein other rows in the table need  
11 not contain sensitive data;  
12 wherein the sensitive object can include one of:  
13 a sensitive table containing sensitive data in the database  
14 system, and  
15 an object that represents a sensitive user of the database system who is  
16 empowered to access sensitive data,  
17 whereby an administrator cannot become a sensitive user and thereby  
18 obtain access to sensitive objects indirectly;  
19 if the object is not a sensitive object, and if the command is received from  
20 a normal database administrator for the database system, allowing the  
21 administrative function to proceed; and

22           if the object is a sensitive object, and if the command is received from a  
23   normal system administrator, disallowing the administrative function.

1           10. (Original) The computer-readable storage medium of claim 9, wherein  
2   the method further comprises:

3           receiving a request to perform an operation on a data item in the database  
4   system;

5           if the data item is a sensitive data item containing sensitive information  
6   and if the request is received from a sensitive user who is empowered to access  
7   sensitive data, allowing the operation to proceed if the sensitive user has access  
8   rights to the data item; and

9           if the data item is a sensitive data item and the request is received from a  
10   normal user, disallowing the operation.

1           11. (Original) The computer-readable storage medium of claim 10,  
2   wherein if the data item is a sensitive data item, if the operation is allowed to  
3   proceed, and if the operation involves retrieval of the data item, the method  
4   further comprises decrypting the data item using an encryption key after the data  
5   item is retrieved.

1           12. (Original) The computer-readable storage medium of claim 11,  
2   wherein the encryption key is stored along with a table containing the data item.

1           13. (Original) The computer-readable storage medium of claim 12,  
2   wherein the encryption key is stored in encrypted form.

1           14. (Canceled).

1           15. (Original) The computer-readable storage medium of claim 9, wherein  
2 if the object is not a sensitive object, and if the command to perform the  
3 administrative function is received from a security officer, the method further  
4 comprises allowing the security officer to perform the administrative function.

1           16. (Original) The computer-readable storage medium of claim 9,  
2 wherein the database system includes a number of sensitive data items;  
3 and  
4 wherein only specific sensitive users are allowed to access a given  
5 sensitive data item.

1           17. (Currently amended) An apparatus for managing a database system,  
2 comprising:  
3 a command receiving mechanism that is configured to receive a command  
4 to perform an administrative function involving an object defined within the  
5 database system;  
6 an execution mechanism that is configured to,  
7 |           determine if the object is a sensitive object that is  
8 |           associated with security functions in the database system, wherein  
9 |           the sensitive object and only the sensitive object is encrypted in the  
10 |           database system, wherein the sensitive object can include a  
11 |           sensitive row within a table in the database system, wherein the  
12 |           sensitive row contains sensitive data, and wherein other rows in the  
13 |           table need not contain sensitive data, wherein the sensitive object  
14 |           can include one of:  
15 |                                    a sensitive table containing sensitive data in  
16 |                                    the database system, and

17 an object that represents a sensitive user of  
18 the database system who is empowered to access  
19 sensitive data.  
20 whereby an administrator cannot become a sensitive user  
21 and thereby obtain access to sensitive objects indirectly;  
22 allow the administrative function to proceed, if the object is  
23 not a sensitive object, and if the command is received from a  
24 normal database administrator for the database system, and to  
25 disallow the administrative function, if the object is a  
26 sensitive object, and if the command is received from a normal  
27 system administrator.

1 18. (Original) The apparatus of claim 17,  
2 wherein the command receiving mechanism is configured to receive a  
3 request to perform an operation on a data item in the database system;  
4 wherein the execution mechanism is configured to,  
5 allow the operation to proceed, if the data item is a  
6 sensitive data item, if the request is received from a sensitive user  
7 who is empowered to access sensitive data, and if the sensitive user  
8 has access rights to the data item, and to  
9 disallow the operation, if the data item is a sensitive data  
10 item, and if the request is received from a normal user.

1 19. (Original) The apparatus of claim 18, further comprising a decryption  
2 mechanism, wherein if the data item is a sensitive data item, if the operation is  
3 allowed to proceed, and if the operation involves retrieval of the data item, the

4 decryption mechanism is configured to decrypt the data item using an encryption  
5 key after the data item is retrieved

1 20. (Original) The apparatus of claim 19, wherein the encryption key is  
2 stored along with a table containing the data item.

1 21. (Original) The apparatus of claim 20, wherein the encryption key is  
2 stored in encrypted form.

1 22. (Canceled).

1 23. (Original) The apparatus of claim 17, wherein if the object is not a  
2 sensitive object, and if the command to perform the administrative function is  
3 received from a security officer, the execution mechanism is configured to allow  
4 the security officer to perform the administrative function.

1 24. (Original) The apparatus of claim 17,  
2 wherein the database system includes a number of sensitive data items;  
3 and  
4 wherein only specific sensitive users are allowed to access a given  
5 sensitive data item.

---